UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,423	03/29/2001	Michael S. Ripley	42390P10855	9405

8791 7590 04/14/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
HAMILTON, MONPLAISIR G	

ART UNIT	PAPER NUMBER
2135	8

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/823,423	RIPLEY ET AL	
	Examiner	Art Unit	
	Monplaisir G Hamilton	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 remain for examination.

Response to Arguments

2. In view of the Appeal Brief filed on 1/30/04, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Objections

3. Claim 8 is objected to because of the following informalities: "the said", line 1, grammatical/typographical error. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear whether applicant has attempted to construct a Markush type claim with regard to Claim 1. The claim is vague as to exactly how the bus key is constructed one reading leads to an interpretation where the bus key is constructed using either a portion of a key distribution data block, a device key or a nonce. Another interpretation requires that the bus key be generated using a portion of a key distribution block and one or more device keys and a nonce. Examiner has interpreted the claim using the broadest interpretation, wherein the bus key is generated using either a portion of a key distribution data block, a device key or a nonce. Please See MPEP 2173.05(h) regarding proper Markush construction.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1-4, 6-9, 11-19, 21-26 are rejected under 35 U.S.C. 102(a) as being anticipated by Content Protection for Recordable Media Specification Revision .94 by IBM et al, herein referred to as IBM.

Referring to Claim 1:

IBM discloses a system comprising: a number generator to generate a nonce (page 5-5, lines 1-6); and an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus (page 5-4, lines 1-10), wherein said encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to said encryption subsystem and the nonce generated by the number generator (page 5-5, lines 1-16; page 6-3-page 6-4).

Referring to Claim 11:

IBM disclose a method comprising: a storage device reading a key distribution data block from a storage medium (page 5-4, lines 1-10); the storage device processing at least a portion of

said key distribution data block using least one device key to compute a media key (page 5-4, lines 4-10); the storage device fetching a nonce generated by a number generator (page 5-5, lines 1-5); the storage device combining said nonce with said media key using a one-way function to generate a bus key (page 5-5, lines 5-20); the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and the storage device transmitting the encrypted data over a data bus (page 5-5, lines 16-25; page 6-3-page 6-4).

Referring to Claim 18:

IBM discloses an apparatus comprising: a storage device to access a storage medium containing data and a key distribution data block, said storage device including a processing logic (Fig 5-1), a one-way function and an encryption logic (Fig 5-1), wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said storage device to compute a media key (page 5-4, lines 4-10), said one-way function combines said media key with a nonce generated by a number generator to produce a bus key (page 5-5, lines 1-22) and said encryption logic encrypts said data accessed from said storage medium using said bus key prior to transmitting the encrypted data via a data bus (page 5-5, lines 16-25; page 6-3-page 6-4).

Referring to Claim 2:

IBM discloses the limitations of Claim 1 above. IBM further discloses a decryption subsystem coupled to said data bus to, decrypt said encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block,

at least one device key assigned to said decryption subsystem and the nonce generated by the number generator (page 5-5-page 5-6, Section 5.2.2).

Referring to Claim 3:

IBM discloses the limitations of Claim 1 above. IBM further discloses said encryption subsystem comprises: a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said encryption subsystem to compute a media key (Fig. 5.1; page 5-4, lines 1-10); a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator (page 5-5, lines 1-20); and an encryption logic to encrypt data accessed from said storage medium using said encryption bus key (page 5-5, lines 16-25).

Referring to Claim 4:

IBM discloses the limitations of Claim 2 above. IBM further discloses said decryption subsystem (Fig 5-1, playback device) comprises: a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said decryption subsystem to compute a media key (page 5-5, lines 28-35); a one-way function to generate the decryption bus key based on said media key and the nonce generated by the number generator; and a decryption logic to decrypt data transmitted over the data bus by using said decryption bus key (page 5-6, lines 1-20).

Referring to Claim 6:

IBM discloses the limitations of Claim 2 above. IBM further discloses said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data (page 3-4, lines 1-10).

Referring to Claim 7:

IBM discloses the limitations of Claim 2 above. IBM further discloses said encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device (Fig. 5-1-Content Encryption and Decryption for the Video Recording Format).

Referring to Claim 8:

IBM discloses the limitations of Claim 2 above. IBM further discloses said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised (Fig 6-3; page 6-3, lines 1-10).

Referring to Claim 9:

IBM discloses the limitations of Claim 2 above. IBM further discloses wherein said storage medium is selected from digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory magnetic card and optical card (Fig. 5-1 and Fig 6-1).

Referring to Claim 12:

IBM discloses the limitations of Claim 11 above. IBM further discloses said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by the storage device to encrypted, said data transmitted over the data bus (page 6-3-page 6-5).

Referring to Claim 13:

IBM discloses the limitations of Claim 11 above. IBM further discloses decrypting the encrypted data received over the data bus (page 5-5-page 6-1).

Referring to Claim 14:

IBM discloses the limitations of Claim 13 above. IBM further discloses said decrypting the encrypted data received over the data bus comprises: a host device reading the key distribution data block from the storage medium (page 5-4); the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key

(page 5-4, lines 4-10); the host device fetching the nonce generated by the number generator (page 5-5, lines 1-10); the host device combining said media key with the nonce using a one-way function to generate a bus key; and the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device (page 5-5, lines 1-25) (Fig 6-1; page 5-5-page 6-1).

Referring to Claim 15:

IBM discloses the limitations of Claim 13 above. IBM further discloses the host device requesting a descramble key required for descrambling scrambled content from said storage device (page 5-5, lines 10-12); the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device (page 5-5, lines 10-18); the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device the host device descrambling said decrypted data using said descramble key decrypted by said host device (page 5-6, lines 8-15) (page 5-5-page 5-6).

Referring to Claim 16:

IBM discloses the limitations of Claim 11 above. IBM further discloses said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data (page 3-4, lines 1-10).

Referring to Claim 17:

IBM discloses the limitations of Claim 14 above. IBM further discloses wherein said number generator is a random number generator residing within the host device (page 5-5, lines 1-10 and page 6-1).

Referring to Claim 19:

IBM discloses the limitations of Claim 18 above. IBM further discloses a host device coupled to said storage device via said data bus, said host device including a processing logic, a one-way function and a decryption logic (Fig 6-1, page 5-4-page 5-5), wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said host device to compute a media key (page 5-4, lines 4-10), said one-way function combines said media key with said nonce generated by said number generator to produce a bus key and said decryption logic decrypts said encrypted data received over the data bus using said bus key (page 5-5, lines 16-25; page 6-3-page 6-4).

Referring to Claim 21:

IBM discloses the limitations of Claim 19 above. IBM further discloses said media key computed by the said storage device will be the same as the media key computed by the host device provided that neither the device key assigned to the storage device nor the device key assigned to the host device have been compromised (page 6-3-page 6-4).

Referring to Claim 22:

IBM discloses the limitations of Claim 19 above. IBM further discloses said number generator is a random number generator residing within said host device (Fig 6-1, page 5-5, lines 1-16).

Referring to Claim 23:

IBM discloses the limitations of Claim 19 above. IBM further discloses said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or a personal computer (Fig 5-1, page 6-1 and Fig 6-1).

Referring to Claim 24:

IBM discloses the limitations of Claim 19 above. IBM further discloses said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card (Fig 5-1, page 6-1 and Fig 6-1).

Referring to Claim 25:

IBM discloses the limitations of Claim 19 above. IBM further discloses said storage medium is embodied in the form of a DVD containing scrambled content (page 5-3, Table 5-4).

Referring to Claim 26:

IBM discloses the limitations of Claim 19 above. IBM further discloses said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data (page 3-2-page 3-3).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by US 6289102 issued to Ueda et al, herein referred to as Ueda.

Referring to Claim 1:

Ueda discloses a system comprising: a number generator to generate a nonce (col 33, lines 55-65); and an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus (col 34, lines 50-65), wherein said encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to said encryption subsystem and the nonce generated by the number generator (col 34, lines 1-45).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5, 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Content Protection for Recordable Media Specification Revision .94 by IBM et al, herein referred to as IBM in view of US 5949881 issued to Davis, herein referred to as Davis.

Referring to Claims 5 and 20:

IBM discloses the limitations of Claim 1 above.

IBM does not explicitly disclose "said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus (col 3, lines)."

Davis disclose said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus (col 3, lines 5-15 and 50-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of IBM such that the random number generator created nonce's that prevent replay attack. One of ordinary skill in the art would have been motivated to do this because it would the random number generated by for the title key can provide the same functionality. Furthermore it would prevent unauthorized access to the content (Davis: Col 3, lines 1-15).

Referring to Claim 10:

IBM discloses the limitations of Claim 2 above.

IBM does not explicitly discloses, "said number generator is a random number generator residing within said decryption subsystem".

Davis discloses said number generator is a random number generator residing within said decryption subsystem (col 3, lines 45-60).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of IBM such that the random number generator is located in the decryption device. One of ordinary skill in the art would have been motivated to do this because it would it would prevent unauthorized access to the content (Davis: col 3, lines 1-15).

Prior Art

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 6301663 issued to Kato, Taku et al. Kato disclose a system that protects the unauthorized copy of multimedia data, recorded on an information recording medium, by using electronic watermark information and key information. The electronic watermark information embedded in the multimedia data is extracted by an electronic watermark extraction unit on the decryption system side. A disk key is obtained using the electronic watermark information and a part master key. The multimedia data is decrypted using the resultant disk key.

US 5915018 issued to Aucsmith, David Wayne. Aucsmith discloses a cryptographic system and method for secure distribution and management of cryptographic keys for use in a DVD copy protection scheme is disclosed. A DVD disc having compressed, encrypted content written on a first portion of the disc, and the content encryption key, itself encrypted with a second key and written out of band on a second portion of the disc is used to provide content, key, and control information to a DVD drive according to the present invention. The DVD drive is coupled to a decompressor and a video controller. The video controller and DVD drive engage in a handshaking protocol in which all of the communication between them is encrypted. After verifying that the video controller is registered and not known to be compromised, the DVD drive passes the content key and control information to the video controller, and the compressed, encrypted content to the decompressor. The content

decompressed by the decompressor is communicated to the video controller where it is decrypted and converted to video signals. The control information instructs the video controller as to whether an optional analog protection scheme should be applied to the video signals prior to delivering the video signals to the display.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monplaisir G Hamilton whose telephone number is (703) 305-5116. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Monplaisir Hamilton